Officer or alternate. Such registering process shall include the recording of: The date the document was received and originated; the classification of the document; the number of copies; the title and description of the document; the disposition and date; the location of the document; and the serial number assigned to the document. For example, the 25th Top Secret document received within the Criminal Division during 1982 could be assigned the following Top Secret control number: CRM–82–0025.

(c) Top Secret accountability registers shall be maintained by each originating and receiving office for all Top Secret documents received or in its custody.

(d) The name and title of all individuals, including stenographic and clerical personnel, to whom information in Top Secret documents has been disclosed, and the date of such disclosure, shall be recorded. The use of a sheet of paper permanently attached to the document concerned may serve as a disclosure record or log for these purposes. Disclosures to individuals who may have had access to containers in which Top Secret infomation is stored need not be recorded on disclosure records. Disclosure records shall be retained for two years after the document concerned is transferred, downgraded or destroyed.

§ 17.112 Inventories.

Top Secret documents and material shall be inventoried at least once annually. Organizations which store large volumes of classified information may limit their annual inventory to documents and material which have been disclosed within the past year. If a storage system contains large volumes of information and security measures are adequate to prevent access by unauthorized persons, the head of the Office, Board, Division or Bureau may submit a request for a waiver of the annual inventory requirement to the Department Security Officer. However, the request must be fully justified to provide a basis for the Attorney General to approve, in writing, the waiver of these annual inventory requirements.

§ 17.113 Accountability of Secret and Confidential information.

Security Programs Managers within all Offices, Boards, Divisions, and Bureaus are responsible for ensuring that accountability procedures for Secret and Confidential information are established within their respective organizations. Such procedures shall be written and shall pertain to Secret and Confidential information originated or received by a Department component; distributed or routed to a subelement of such component; and disposed of by the component by transfer of custody or destruction. Copies of written procedures for the accountability and control of Secret and Confidential information shall be forwarded to the Department Security Officer. At a minimum, such procedures shall provide for the identification of the document.

§ 17.114 Accountability of reproduced documents.

Reproduced copies of Top Secret, Secret and Confidential documents are subject to the same accountability and controls as the original documents. (See § 17.100(b).)

§ 17.115 Working papers.

''Working papers'' are classified documents and material accumulated or created in the preparation of finished documents and material. Working papers containing classified information shall be dated when created; marked with the highest classification of any information contained therein; protected in accordance with the assigned classification; destroyed when no longer needed; and marked with a declassification or review date when placed in permanent files. Working papers shall be accounted for and controlled in the manner prescribed for a finished document of comparable classification when released by the originator or transmitted through message center channels; filed permanently; or retained more than 180 days from date of origin.

Subpart H—Disposal and Destruction of Classified Information

§17.116 Policy.

All National Security Information shall be destroyed in a manner described herein whenever the operational or historical need for the particular classified information ceases to exist. Every effort shall be made to destroy National Security Information as soon as practical for two basic reasons:

(a) First, the longer large volumes of National Security Information are existent, the greater the potential for compromise.

(b) Second, the physical and document security requirements involving National Security Information are expensive to fulfill and maintain. The smaller the amount of National Security Information in existence within the Department, the fewer storage containers and security areas are required and the smaller the budgetary allotment which must be allocated by the Department to fulfill security requirements.

§17.117 Record material.

Documentary record material made by an Office, Board, Division or Bureau of the Department in connection with the transaction of public business, and preserved as evidence of the organization, functions, policies, operations, decisions, procedures, or other activities of any Department or Agency of the government, may be disposed of or destroyed only in accordance with Offices, Boards and Divisions (OBD) Order 2710.3A, Chapter 6.

§17.118 Nonrecord material.

Nonrecord material containing classified information (including shorthand notes, used carbon paper, one-time typewriter ribbons, word processor disks, preliminary drafts, plates, records and tapes, stencils, negatives, and the like, and wastage incidental thereto) shall be destroyed, in accordance with this subpart, as soon as it has served its purpose, unless it is the subject of an ongoing mandatory review for declassification request. Prior to destruction, this material must be protected in a manner to prevent unauthorized disclosure of the information in accordance with the safeguarding procedures contained in this regulation.

§17.119 Methods of destruction.

Top Secret, Secret and Confidential classified information and material (record and nonrecord) shall be destroyed in the presence of an appropriately cleared official by burning, melting, chemical decomposition, pulping, pulverizing, shredding or other mutilation sufficient to preclude recognition or reconstruction of the classified information. Classified information stored on floppy disks or other forms of magnetic media can also be destroyed by erasure but only when unclassified information is substituted in its place.

§17.120 Records of destruction.

(a) Records of destruction are required for Top Secret and Secret information and shall be dated and signed by two officials (destruction and witnessing officials) witnessing actual destruction. If destruction is accomplished by an approved central disposal system, the destruction record shall be signed by the witnessing officials at the time the material is delivered at the facility. Records of destruction shall be maintained for a minimum of two years after which they may be destroyed. Such records shall contain the identification of the document(s) destroyed, the method of destruction used, the time and place of destruction, the reason for destruction, and the name of the destroying official and witness.

(b) The Security Programs Manager, his/her appointed Security Officer(s) when appropriate, Top Secret Control Officers or their alternates, or custodians of classified information, are authorized to destroy National Security Information. An additional person, who possesses a security clearance at the same or higher level than the classification of the material being destroyed, shall witness the destruction thereof. The destruction officials shall be trained in the operation of the equipment being used for destruction and shall ensure that destruction is accomplished in accordance with provisions of this subpart.